THREAT INTELLIGENCE DATA FEED

GAIN TIMELY, HIGH QUALITY INTELLIGENCE AT YOUR FINGERTIPS

Cyber threats have become the most common and serious threats to enterprises. Last year Blueliv discovered and analyzed more than 2,000,000 crime servers and attackers are escalating and precisely targeting clients with frightening efficiency.

Through Blueliv Threat Intelligence Data Feed clients are armed with the ultra-fresh analysis and data needed to protect their assets from the gamut of online threats. Blueliv Cyber Threat Intelligence Data Feed allows any organization to track in real-time the threats that are aligned against it and to quantify and qualify what attack vectors malicious attackers are using.

Every second, Blueliv scours and analyzes hundreds of sources to turn global threat data into targeted, predictive and actionable intelligence that detects, identifies, and helps stop cyber threats. Furthermore, our security experts are able to view threats and attacker characteristics from an unconventional perspective to successfully anticipate intentions and potential outcomes.

Blueliv's Data Feed provides unique intelligence about verified online crime servers conducting malicious activity, infected bot IPs, malware hashes, attacking IPs and hacktivism activities.

The Feed is offered as an easy to buy solution that provides automated security and high-impact results rapidly. The user can understand what attack vectors malicious actors are using, understand potential indicators of compromise (IOC) and deploy mitigation solutions.

The Data Feed provides organizations with the volume, velocity and variety of real-time threat intelligence needed in order to allow them take decisive actions on the intelligence provided and stay ahead of the cyber threat curve.

The Data Feed is relevant to all industry verticals: financial services, insurance, telecom, utility, government, transport, retail organizations, service providers and security vendors.

Unique intelligence about crime servers, infected bot IPs, malware hashes, hacktivism activities and attacking IPs.

"What part of the threat landscape are you seeing? What blind spots do you have in your intelligence fabric?"

HIGHLIGHTS

- Provides real-time detailed information of a comprehensive range of cyber threats giving organizations the power to define tactical and strategic responses and removing their blind spots in their security fabric.
- Focuses on malicious URLs like botnets C&C (related to bankers, POS, grabbers, ransom), exploit kits or phishing.
- Provides access to open, private and proprietary sources: sinkholed sites, malware repositories, black markets, social media networks, crime servers and alliances.
- Adds intelligence to security controls for an adaptive and automated protection.
- Offers full API access and plugins to integrate the feed with other security systems.
- Supports STIX / TAXII to enable easy information - sharing and collaboration.
- Offered as a monthly subscription service. Unlimited number of queries.

INTELLIGENCE AND DATA PROVIDED – FEEDS

Bot IP:
Infected IPs, OS affected, user agent.
IP address, geolocation type, version, status...

Malware:
Malware hashes, families.

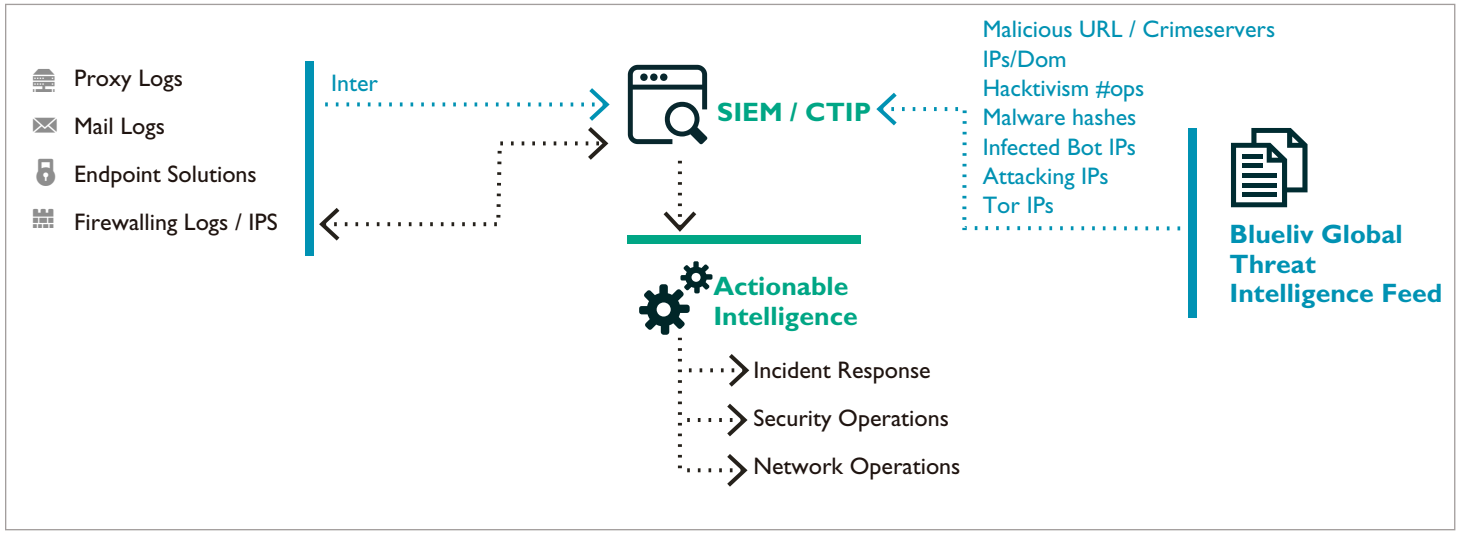
Attacking IPs:
Data related to IPs that are performing attacks like port scan, brute force, directory scan...

Crime servers:
Malware distribution domains, C&Cs, phishing, exploit kits and backdoors. ID, type, country, domain, geolocation, ASN ID, status...

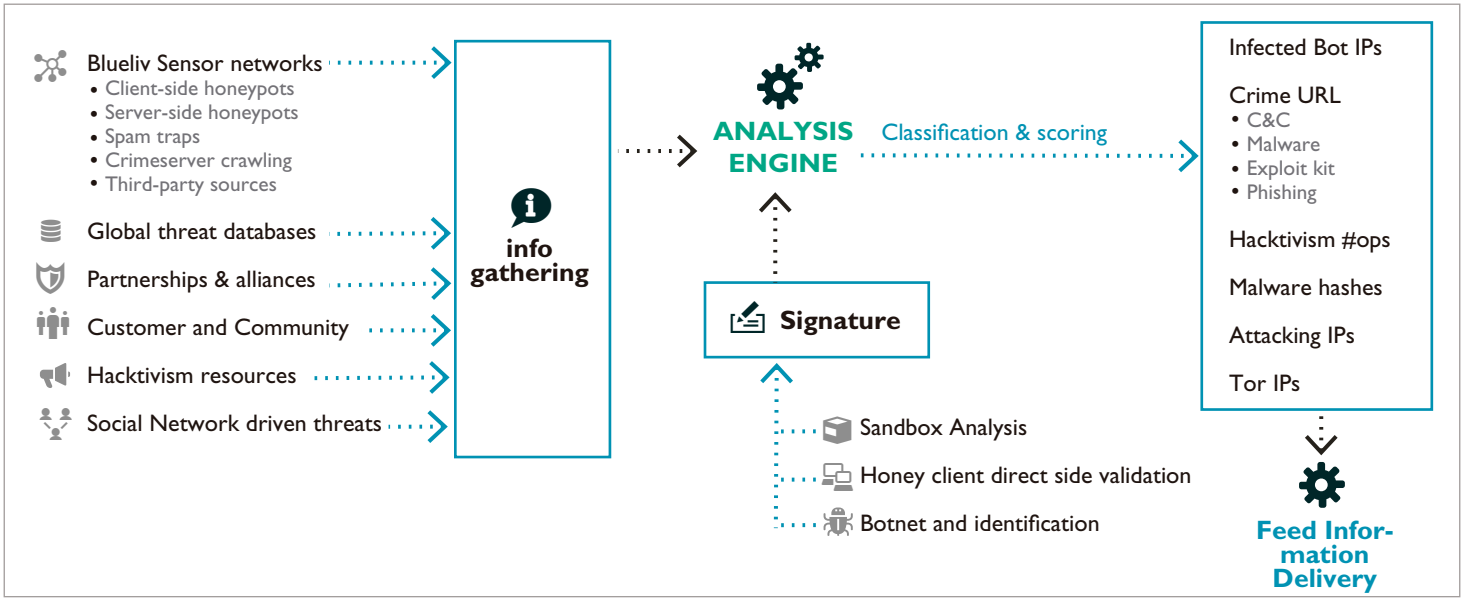
Hacktivism:
Social monitoring related to hacktivism operations.
Ops/Hashtag, country, # tweets per day, tweets.

Tor IP:
Track & discover Tor Exit Nodes

ADDING INTELLIGENCE TO YOUR SECURITY TOOLS



HOW IT WORKS



CAPABILITIES

Use Threat Intelligence Data Feed to build a holistic and adaptive security infrastructure that will result in:

GLOBAL THREAT INTELLIGENCE DELIVERED LOCALLY

Intelligent threat identification achieved through the use of a combination of malware sandboxes, honey pots, honey clients and spam mailboxes that allows companies to identify different threat actors around the world.

CONTINUOUS REAL-TIME UPDATES

The Blueliv feed is constantly tracking threats and these are updated in real-time and providing our clients with ultra-fresh intelligence on live threats targeting their users and customers and enabling security analysts to identify clear IOCs. In addition, the crowd-sourced information helps the clients reduce the false positive ratio. Unlimited queries can be run in real-time.

UNIQUE COMPREHENSIVE RANGE OF CYBER THREAT INTELLIGENCE

The feed provides data relating to crime servers, Bot IP, malware hashes, attacking IPs from honeypots and hacktivism. All that intelligence aggregates data that comes from a wide range of open sources and includes private and proprietary intelligence coming from sinkholed sites, malware repositories and the alliances and collaborations with different organizations.

MACHINE-READABLE THREAT INTELLIGENCE

The Data has been translated from human to machine-readable formats to allow for rapid dispersion to cloud and on-premises infrastructure and through this the client can increase threat visibility and improve their security posture by enhancing threat context. Blueliv supports STIX/TAXII to represent structured cyber threat information and to enable easy information-sharing. Feeds are also available using REST architecture with HTTP protocol and JSON format.

EASY AND DIRECT IMPLEMENTATION

Easy to setup, easy to integrate quickly into your SIEM, firewall, IPs and other security products through a single point of contact (API) or through official security vendor applications markets. Plugins available for Splunk, AlienVault, ArcSight and Logstash and a powerful SDK for integration.

WHAT CAN BLUELIV'S DATA FEED DO FOR YOUR ENTERPRISE?

- Make smart use of scarce internal security resources.
- Ingest large volumes of global intelligence.
- Achieve the 3 V's of threat intelligence, Volume, Varity, Velocity, and move towards strategic threat intelligence.
- No additional software is needed.

TRIAL

Ask for a 14-day trial and test the Threat Intelligence Data Feed.

ABOUT BLUELIV

Blueliv is a leading provider of targeted cyber threat information and analysis intelligence for large enterprises, service providers, and security vendors. Its cyber threat platform and feed addresses a comprehensive range of cyber threats to turn global threat data into predictive, actionable intelligence that detects, identifies, and helps stop cyber threats. Blueliv's clients include leading bank, insurance, telecom, utility, and retail enterprises in Europe, and the company has alliances with leading security vendors and other organizations to share cyber intelligence. Blueliv was named Gartner 2015 Cool Vendor.

www.blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv

plus.google.com/+Blueliv